

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method of electronic document retention, comprising:

assigning a document retention policy to the electronic document, the document retention policy being based on a future event that is unscheduled; and
cryptographically associating, by encrypting at least a portion of the electronic document using a cryptographic key, the document retention policy with the electronic document, wherein the cryptographic key is a document retention key or a key encrypted with a document retention key, and wherein the cryptographic key is protected by a document access policy comprising access rules which provide restrictive access to the cryptographic key and the electronic document.

2. (Previously Presented) The method as recited in claim 1, further comprising:

determining whether the future event has occurred; and
cryptographically preventing access to the electronic document in accordance with the document retention policy based on the occurrence of the future event.

3. (Previously Presented) The method as recited in claim 2, wherein the determining is performed periodically.

4. (Currently Amended) The method as recited in claim 2, wherein the determining comprises interacting with a network accessible resource, wherein the network accessible resource is one or more of a server, an application, a client computing device, or a storage devicesystem.

5. (Currently Amended) The method as recited in claim 2, wherein the determining comprises interacting with a web accessible resource, wherein the web accessible resource is one or more of a web server, an application, a client computing device, or an external storage devicesystem.

6. (Previously Presented) The method as recited in claim 5, wherein the determining comprises:

supplying a future event description of the future event to the web accessible resource; and

determining, at the web accessible resource, whether the future event has occurred.

7. (Previously Presented) The method as recited in claim 6, wherein said supplying is achieved by a universal resource locator associated with the future event description.

8. (Previously Presented) The method as recited in claim 5, wherein the determining comprises:

supplying the future event description to a contract management system;

and

determining, at the contract management system, whether the future event has occurred.

9. (Previously Presented) The method as recited in claim 1, wherein the document retention policy specifies a document retention period based on the future event.

10. (Previously Presented) The method as recited in claim 9, wherein the document retention policy specifies a document retention period that expires a predetermined period of time after the occurrence of the future event.

11. (Previously Presented) The method as recited in claim 9, further comprising:

deactivating the cryptographic key in response to determining that a document retention period has expired, thereby preventing further access to the electronic document.

12. (Previously Presented) The method as recited in claim 11, further comprising:

permitting the deactivating to be overridden so that the electronic document can remain accessible even after the document retention period.

13. (Withdrawn) A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data;

obtaining a document key;

encrypting the data portion of the electronic document using the document key to produce an encrypted data portion;

obtaining a retention access key, the retention access key being used to enforce a document retention policy on the electronic document;

encrypting the document key using the retention access key to produce an encrypted document key;

forming a secured electronic document from at least the encrypted data portion and the encrypted document key; and

storing the secured electronic document.

14. (Withdrawn) The method as recited in claim 13, wherein the retention access key is a public retention access key.

15. (Withdrawn) The method as recited in claim 13, wherein the document retention policy is dependent on a future event that is presently unscheduled, and the

retention access key is used to enforce the document retention policy on the electronic document.

16. (Withdrawn) The method as recited in claim 15, wherein the retention access key is subsequently available from a remote key store only so long as a document retention period of the document retention policy has not been exceeded.

17. (Withdrawn) The method as recited in claim 16, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

18. (Withdrawn) The method as recited in claim 17, wherein said method further comprises:

extending the predetermined period of time after the occurrence of the future event.

19. (Withdrawn) The method as recited in claim 16, wherein said method is performed on a client machine that operatively receives the retention access key from the remote key store over a network.

20. (Withdrawn) A method for accessing a secured electronic document by a requestor, the secured electronic document having at least a header portion and a data portion, said method comprising:

obtaining a retention access key, the retention access key being used to enforce a document retention policy on the electronic document;

obtaining an encrypted document key from the header portion of the secured electronic document;

decrypting the encrypted document key using the retention access key to produce a document key;

decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion; and

supplying the data portion to the requestor.

21. (Withdrawn) The method as recited in claim 20, wherein the retention access key is identified by an indicator within a header portion of the secured electronic document.

22. (Withdrawn) The method as recited in claim 20, wherein the retention access key is a private retention access key.

23. (Withdrawn) The method as recited in claim 20, wherein, the obtaining a retention access key comprises obtaining the retention access key from a server, wherein the server determines whether the retention access key is permitted to be provided to the requestor based on the document retention policy.

24. (Withdrawn) The method as recited in claim 20, wherein the document retention policy is dependent on a future event that is presently unscheduled, and the retention access key is used to enforce the document retention policy on the electronic document.

25. (Withdrawn) The method as recited in claim 20, wherein the retention access key is available only so long as a document retention period of the document retention policy has not been exceeded.

26. (Withdrawn) The method as recited in claim 25, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

27. (Withdrawn) The method as recited in claim 20, wherein the retention access key is available from a remote key store only so long as a document retention period of the document retention policy has not been exceeded.

28. (Withdrawn) The method as recited in claim 20, wherein the retention access key is available only so long as a document retention period of the document retention policy has not been exceeded, the document retention period can be extended to permit extended access to the electronic document.

29. (Currently Amended) A computer-implemented method for distributing cryptographic keys used in a file security system, said method comprising:

receiving, at a computing device, a request for a document retention key that is necessary to gain access to a cryptographically secured electronic document;

identifying, by the computing device, a document retention period having been cryptographically associated with the secured electronic document by encrypting at least a portion of the secured electronic using the document retention key and, the document retention period being dependent on a future event that was unscheduled when the document retention period was associated with the secured electronic document, wherein the document retention key is protected by a document access policy comprising access rules which provide restrictive access to the cryptographic key and the secured electronic document;

determining, by the computing device, whether the document retention period associated with the document retention key has been exceeded; and

refusing to distribute the document retention key in response to determining that the document retention period for the electronic document has been exceeded.

30. (Previously Presented) The computer-implemented method as recited in claim 29, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

31. (Previously Presented) The computer-implemented method as recited in claim 29, wherein said computing device is a server, and wherein the request for the document retention key is from a client module that is connectable to the server via a network.

32. (Previously Presented) The computer-implemented method as recited in claim 29, wherein the document retention period can be extended to permit extended access to the electronic document.

33. (Currently Amended) A file security system comprising:

a processor;

a memory having instructions stored thereon, that, in response to execution by the processor, cause the processor to restrict access to electronic files, the instructions comprising:

instructions for storing a plurality of cryptographic key pairs in a key store, each of the cryptographic key pairs including a public key and a private key, at least one of the cryptographic key pairs pertaining to a retention policy, the retention policy being dependent on a future event, wherein the cryptographic key pairs are document retention keys or keys encrypted with a document retention key, and wherein the cryptographic key pairs are protected by a document access policy comprising access rules which provide restrictive access to the cryptographic key pairs and the electronic files; and

instructions for determining whether the private key of the at least one of the cryptographic key pairs pertaining to the retention policy is permitted to be provided to a requestor based on whether the future event has occurred,

wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the retention policy to access a secured electronic file, and wherein the secured electronic file was previously cryptographically associated with the retention policy by encrypting at least a portion of the secured electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy, and at the time the electronic file was so secured, the future event was unscheduled.

34. (Previously Presented) The file security system as recited in claim 33, wherein the instructions for determining comprise instructions for preventing the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from being provided to the requestor after a predetermined retention period following the occurrence of the future event.

35. (Previously Presented) The file security system as recited in claim 33, wherein the requestor is a client module that operatively connects to said access manager over a network.

36. (Previously Presented) The file security system as recited in claim 33, wherein said file security system further comprises:

at least one client module configured to assist in selecting the retention policy and secure the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy so as to cryptographically impose the retention policy.

37. (Previously Presented) The file security system as recited in claim 33, wherein said file security system further comprises:

at least one client module, said client module assisting with unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertains to the retention policy from said key store if permitted by said access manager, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertains to the retention policy.

38. (Currently Amended) A non-transitory computer readable medium having computer-executable instructions stored thereon for providing data retention for electronic data, the computer-executable instructions comprising:

instructions to assign a data retention policy to the electronic data, the data retention policy being based on a future event that is unscheduled; and

instructions to cryptographically associate, by using a cryptographic key to encrypt at least a portion of the electronic data, the data retention policy with the electronic data, wherein the cryptographic key is a document retention key or a key encrypted with a document retention key, and wherein the cryptographic

key is protected by a document access policy comprising access rules which provide restrictive access to the cryptographic key pairs and the electronic data.

39. (Previously Presented) The computer readable medium as recited in claim 38, wherein the instructions further comprise:

instructions to cryptographically prevent access to the electronic data in accordance with the data retention policy based on the occurrence of the future event.

40. (Previously Presented) The computer readable medium as recited in claim 39, wherein the electronic data is an electronic file.

41. (Previously Presented) The computer readable medium as recited in claim 39, wherein the electronic data is an electronic document.

42. (Previously Presented) The computer readable medium as recited in claim 38 wherein

the data retention policy specifies a data retention period based on the future event.

43. (Previously Presented) The computer readable medium as recited in claim 42 wherein:

the data retention policy specifies a data retention period that expires a predetermined period of time after the occurrence of the future event, and the instructions further comprise:

instructions to determine whether the data retention period has expired; and

instructions to deactivate the cryptographic key in response to determining that the data retention period has expired, thereby preventing further access to the electronic data.

44. (Previously Presented) The computer readable medium as recited in claim 43, wherein the instructions further comprise:

instructions to permit deactivation of the cryptographic key to be overridden so that the electronic data can remain accessible even after the data retention period.

45. (Previously Presented) The method as recited in claim 4, wherein the determining comprises:

supplying a future event description of the future event to the network accessible resource; and

determining, at the network accessible resource, whether the future event has occurred.

46. (Withdrawn) The method as recited in claim 16, wherein said method is performed on a server that operatively receives the retention access key from the remote key store over a network.